WK:MJB
F. #2019R01483

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF A GOOGLE PIXEL 3, SERIAL NUMBER 89UX0GJH8, IMEI 358275090560760, CURRENTLY LOCATED IN THE EASTERN DISTRICT OF NEW YORK	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. 20-MJ-55

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Matthew Deragon, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been employed as a Special Agent since 2014, and I am currently assigned to the Criminal Division of New York. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I am now assigned to the FBI's Violent Crimes against Children Squad (the "Squad"), which investigates individuals suspected of being involved in the online sexual

exploitation of children. As part of my duties as a member of the Squad, I investigate violations relating to child exploitation and child pornography, including violations pertaining to the production, possession, distribution, and receipt of child pornography as well as the enticement of minors to engage in illicit sexual conduct, in violation of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422 and 2423. I have received training in investigating child pornography and child exploitation, and I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256[1]) in all forms of media, including computer media. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is intended to show only that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a Google Pixel 3, Serial Number 89UX0GJH8, IMEI 358275090560760, hereinafter the "DEVICE." The DEVICE is currently in federal law enforcement custody within the Eastern District of New York.

[1] "'[C]hild pornography' means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where—(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct."

5. The applied-for warrant would authorize the forensic examination of the DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B that relate to violations of Title 18 United States Code, Sections 2251, 2252, 2252A, 2422 and 2423.

PROBABLE CAUSE

6. In or about October, 2019, law enforcement learned that Aaron Weinreb (hereinafter "Defendant"), age 48, had engaged in oral and anal sex with a fifteen-year-old minor (hereinafter "Victim") on multiple occasions.[2] The relationship between the Defendant and the Victim began when the Victim was fourteen years old.

7. Law enforcement met with the Victim and reviewed the Victim's cell phone activity with the Defendant. The Victim indicated that the Defendant communicated using the cell phone number 917-722-0268. I learned that 917-722-0268 was a temporary phone number attributed to Talkatone.[3] A subpoena to Talkatone identified that the IP address 68.198.2.251 was used to log into Talkatone and access the temporary phone number, 917-722-0268. A subpoena to Optimum Online revealed that the IP address 68.198.2.251 was subscribed to the Defendant, Aaron Weinreb, at 310 Eastwood Road, Woodmere, New York. Text messages between the Defendant and the Victim, obtained from the Victim's cell phone, corroborated that the Defendant communicated with the

[2] On October 30, 2019, the Defendant was charged under Criminal Complaint 19-1014-M with enticement of a minor in violation of 18 U.S.C. § 2422(b). On January 8, 2020, a grand jury returned indictment 20-CR-006 (BMC) charging the Defendant with two counts of coercion and enticement of a minor to engage in illegal sexual activity, in violation of 18 U.S.C. § 2422(b).

[3] TalkTone is an Internet application which allows users to send and receive free voice calls and messages.

Victim using the phone number 917-722-0268, and that the Defendant had engaged in sexual activity with the Victim.

8. On or about May 18, 2019, within days of engaging in sexual activity with the Victim, the Defendant sent a text message from phone number 917-722-0268 that stated, "I was trying to demonstrate what our relationship probably is.. an older taking advantage of a vulnerable child.. I'm sorry. I didn't mean to hurt you."[4]

9. On or about May 22, 2019, the Defendant sent a text message from phone number 917-722-0268 that boasted, "I was strong last time.. but i was just showing you what an older guy does when he is so excited and sexually aroused."

10. Later that same day, May 22, 2019, the following text exchange occurred between the Defendant and the Victim:

> Defendant: "I want you to give me the love I crave… Not anal sex.. but a loving sexual relationship in every other way.. that's the truth.. please be honest about if you want that too"
>
> Victim: "I want that too, not every time we meet has to be about sex"
>
> Defendant: It's not.. I think we found a nice balance.. I love when we kiss and I hope you will see how nice it is to deep kiss and really feel the warmth of each other's mouth.. but cuddling for adults means being touched and held in sexual parts and getting aroused.. its not like getting a hug from your mom .."

11. On or about October 9, 2019, the FBI assumed the electronic identity of the Victim and continued communicating with the Defendant at 917-722-0268. Law

[4] Typographical errors appear in the original text of the messages, and have therefore not been corrected in the search warrant application.

enforcement used the same cell phone number the Victim had previously used to communicate with the Defendant.

12. On or about October 24, 2019, the Defendant, using phone number 917-722-0268, texted the Victim and stated, "I do love when you suck my dick and when we cuddle your dick is always…solid hard"

13. On or about October 24, 2019, using the Victim's cellphone number, the FBI messaged the Defendant and asked him to communicate using a private text application. The Defendant agreed to use the private text application, and did so using cell phone number 917-722-0268, which is the same number he previously used to electronically communicate with the Victim.

14. Using cell phone number 917-722-0268 on the private text application, the Defendant expressed a desire to meet the Victim on Tuesday, October 29, 2019. On October 24, 2019, the Defendant and the Victim (FBI) exchanged text messages, including the following:

Victim (FBI): "My parents have been so annoying lately"

Defendant: "Lol, I would be too if I had a 16 year old"

Victim (FBI): "Yea"

Defendant: "Just finished work..I assume not today?"

Victim (FBI): I'm sorry, just still sick"

Defendant: "I don't mind . But no worries.. But then maybe Tuesday afternoon"

Victim (FBI): "Yes Tuesday but I have school stuff into the afternoon"

15. On October 24, 2019, the Defendant sent the Victim (FBI) messages, using the private text application from phone number 917-722-0268, that stated, "I want to cuddle with you and feel your hard dick pressed up against me while we snuggle" and "I want to kiss you now..I can't wait till Tuesday"

16. On October 29, 2019, the Defendant texted the Victim (FBI) from phone number 917-722-0268 and indicated, in sum and substance, that he reserved a hotel room at the King's Hotel in the vicinity of 8th and 39th Street in Brooklyn New York. Law enforcement responded to the Kings Hotel, 820 39th Street, Brooklyn, NY 11232, where they detained the Defendant, seized the DEVICE and provided Miranda warnings twice.

17. The Defendant acknowledged his Miranda warnings and agreed to speak with law enforcement. The Defendant initially indicated he was a doctor and that he was at the hotel for a nap. When questioned about a fifteen year old boy that was waiting to meet with him, the Defendant requested a lawyer. Shortly thereafter, not in response to questioning, the Defendant asked questions to members of law enforcement and made statements about the investigation. Law enforcement again provided Miranda warnings and the Defendant agreed to speak with law enforcement without counsel.

18. During questioning, the Defendant admitted to having oral sex with the Victim at a time when he knew the Victim was sixteen years old. The Defendant further admitted to having oral sex with another sixteen year old male, after having met him using the geosocial networking and online dating application, Grinder. Multiple times during the interview, the Defendant asserted that he had a sex addiction.

19. The Defendant voluntarily gave law enforcement the DEVICE. During the Defendant's interview, law enforcement called cell phone number 917-722-0268, and the DEVICE exhibited a missed call or "alert" as a result of law enforcement's call.

20. The DEVICE is currently in the possession of the FBI, within the Eastern District of New York, as we seized it on October 29, 2019 when the Defendant gave it to us.

21. Based upon my training and experience, I know that the DEVICE has been stored in a manner in which its contents are in substantially the same state as they were when the DEVICE first came into the possession of the FBI.

TECHNICAL TERMS

22. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and

downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24

NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

23. Based on my training, experience, and research, I know that the DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or

suggests who possessed or used the device as well as evidence of communication with and enticement of minors in violation of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422 and 2423.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on devices. This information can sometimes be recovered with forensics tools.

25. There is probable cause to believe that things that were once stored on the DEVICE may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. As a result of the above, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, a device's internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to communicate with and illegally entice a minor victim, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the DEVICE to human inspection in order to determine whether it is evidence described by the warrant. The examination may also require the use of programs or applications designed to circumvent or break protective passcodes on the DEVICE.

28. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

29. I submit that this affidavit provides probable cause for a search warrant authorizing the examination of the DEVICE described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

MATTHEW D. DERAGON
Special Agent, Federal Bureau of Investigation

Subscribed and sworn to before me
on January 15, 2020:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a Google Pixel 3, Serial Number 89UX0GJH8, IMEI 358275090560760, hereinafter the "DEVICE." The DEVICE is currently in federal law enforcement custody within the Eastern District of New York.

This warrant authorizes the forensic examination of the DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the DEVICE described in Attachment A that relate to violations of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422 and 2423 and involve the Defendant, Aaron Weinreb, since 2018, including:

a. All forms of communication with sexual exploitation victims or potential victims; and

b. Evidence of user attribution showing who used or owned the DEVICEs at the time the things described in this warrant were used, created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.